ETSI GR NFV-SEC 007 V1.2.1 (2024-11)

Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
RGR/NFV-SEC007ed121

Keywords
ICT, NFV, security, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definition of terms, symbols and abbreviations 7
3.1 Terms 7
3.2 Symbols 7
3.3 Abbreviations 7
4 Attestation Procedures 7
4.0 Introduction 7
4.1 Basic Concepts 7
4.1.1 Roots of Trust 7
4.1.1.1 Overview 7
4.1.1.2 Hardware Based Root of Trust 8
4.1.1.3 RoT for virtualised platforms 8
4.1.1.4 Security services of RoTs 8
4.1.2 Chain of Trust 8
4.1.3 Attestation 10
4.1.4 Supporting Technologies 10
4.1.4.1 Measured Boot 10
4.1.4.2 Load-Time Measurement 11
4.2 Enforcement of System Integrity 11
4.3 Trustworthy Platform Configuration 12
4.4 Remote Attestation of VNFs 13
4.4.1 Introduction 13
4.4.2 Known Challenges 14
4.4.3 Single-Channel VM-Based Deep Attestation 15
4.4.4 Multiple-Channel Independent Deep Attestation 15
5 Levels of Assurance 16
5.0 Introduction 16
5.1 Attestation and Assurance 17
5.1.0 Introduction 17
5.1.1 Platform Attestation 18
5.1.2 Virtual Machine Attestation 18
6 Infrastructure Capabilities 18
6.0 Introduction 18
6.1 Roots of Trust 18
6.1.1 Overview 18
6.1.2 Root of Trust for Measurement 19
6.1.3 Root of Trust for Storage 19
6.1.4 Root of Trust for Reporting 19
6.1.5 Examples of implementation of Roots of Trust 19
6.1.5.1 Trusted Platform Module 19
6.1.5.2 Hardware Security Module 20
6.1.5.3 Hardware Co-Processors, Chipset, Processor Modes 21
6.2 Measured Boot 21
6.3 OS Measurement Architecture 21
6.4 Secure Boot 21
6.5 OS Enforcement of Integrity 22
6.6 Remote Attestation 22

6.7 Other Capabilities 22
6.8 Levels of Assurance to Capabilities Mapping 22

7 Operational Procedures 23
7.0 Introduction 23
7.1 Platform Deployment 23
7.1.1 Deployment Specific Processes 23
7.1.2 Mutual Key Registration 24
7.1.2.1 Attestation Key Generation 24
7.1.2.2 Attestation Key Registration 24
7.1.2.3 Remote Verifier Secure Channel 24
7.1.3 Golden measurements registration 25
7.2 Attestation Cycle 25
7.2.1 Attestation flow 25
7.2.2 Attestation intervals 26

8 Analysis of the Evolution of Attestation Technologies 26
8.1 Network Service (NS) Attestation 26
8.2 Infrastructure Network Attestation Using a SDN Verifier 27
8.3 Perspectives for Run-Time Attestation 28
8.4 Attestation using HMEE based technology 29

Annex A: Possible Proof of Concepts 30

Annex B: Change history 31

History 32

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G logo** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document discusses existing attestation technologies and practices, as applicable to NFV systems, addressing:

- The identification and definition of levels of assurance
- The assumed capabilities from the NFVI (e.g. TPM, HSM, etc.)
- Operational procedures
- A gap analysis of current (established or newly proposed) attestation technologies
- Recommendations for follow-on PoCs to demonstrate feasibility of the attestation procedures

Given the current status of attestation technologies and standards, the present document is applicable to hypervisor-based NFV deployments only, with the exception of some of the perspectives analysed in clause 8.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.2] ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".

[i.3] ETSI GS NFV-SEC 012: "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[i.4] TCG, PC Client WG: "PC Client Specific Implementation Specification for Conventional BIOS", V1.21 Errata, rev 1.0, 2012-02.

[i.5] TCG, Infrastructure WG: "TCG Attestation, PTS Protocol: Binding to TNC IF-M", V1.0, revision 28, 2011-08.

[i.6] ETSI GR NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".

[i.7] ETSI GR NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[i.8] Unified Extensible Firmware Interface Forum: "Unified Extensible Firmware Interface Specification", V2.7, 2017-05.

[i.9] NIST SP800-155, draft, 2011-12: "BIOS Integrity Measurement Guidelines".

[i.10] TCG PC Client WG: "TCG EFI Platform Specification", V1.22, revision 15, 2014-01.

[i.11] TCG Virtual Platform WG: "Virtualised Trusted Platform Architecture Specification", V1.0, revision 0.26, 2011-09.

[i.12] TCG TPM WG: "Trusted Platform Module Library Specification", V1.38, 2016-09.

[i.13] Andre Rein, 2017: "DRIVE: Dynamic Runtime Integrity Verification and Evaluation", Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms and definitions given in ETSI GR NFV 003 [i.1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR NFV 003 [i.1] and the following apply:

CoT	Chain of Trust
CRTM	Core Root of Trust for Measurement
HBRT	Hardware Based Root of Trust
LoA	Level of Assurance
RoT	Root of Trust
SML	Stored Measurement Log

4 Attestation Procedures

4.0 Introduction

Both authentication (a process of ensuring that the computing platform can prove that it is what it claims to be) and attestation (a process of proving that a computing platform is trustworthy and has not been breached) are necessary steps to ensure secure computing in NFV environment. Attestation procedures create assurances of computing platform's integrity state and ability to protect data in accordance with policy.

4.1 Basic Concepts

4.1.1 Roots of Trust

4.1.1.1 Overview

The trust status of a computing platform can be determined by a remote party only by using inherently trusted primitives embedded into that platform. These primitives are called Roots of Trust (RoTs). The RoTs are expected to behave always according to their predefined purpose, as no other mechanism is available to fully check their behaviour.

The RoTs are ideally implemented in hardware or protected by hardware mechanisms and provide very specific services to the computing platform they are serving. For attestation of a computing platform, three main services types are required to be supported by its RoTs:

- Protection of cryptographic material (e.g. keys).
- Isolated execution of cryptographic operations.
- Bootstrapping code measurement.

4.1.1.2 Hardware Based Root of Trust

In NFV deployments it is expected that the virtualisation layer (i.e. hypervisor) will make use of a Hardware Based Root of Trust (HBRT). The HBRT should be implemented in a hardware component that fulfils the requirements defined in ETSI GS NFV-SEC 012 [i.3]. The HBRT provides a subset of the services required for enabling a remote party to compute the trust status of the virtualisation host.

4.1.1.3 RoT for virtualised platforms

Unlike the virtualisation layer, which is expected to run directly on the hardware of the compute node, the VNFCIs will run on virtualised platforms. They may run in an execution environment created by the hypervisor based on dedicated hardware support.

The same principle applies to the RoTs available to the virtualised platform: the virtual platform can make use of dedicated hardware features provided by the HBRT (as defined in ETSI GS NFV-SEC 012 [i.3]), but the hypervisor is involved in configuring this access and sometimes transferring messages between VNFCIs and their associated hardware rooted vRoTs. Therefore, a vRoTs represents the combination of hardware functionality provided by the HBRT and the relevant components of the hypervisor that configure and mediate access to those functionalities.

In NFV deployments, it is highly desirable to restrict as much as possible the influence of the hypervisor on the vRoTs. Coupled with the host hardening requirements of ETSI GS NFV-SEC 012 [i.3], this would ensure the best available protection for the vRoTs.

If HMEE technology is used to host and protect virtual RoTs, one possibility to integrate them in the CoT is to tether them to their corresponding HBRT implementation (e.g. TPM, HSM, etc.).

4.1.1.4 Security services of RoTs

A RoT provides one or more security services to the platform, e.g. software measurement service for the Root of Trust for Measurement (RTM), software measurement and measurement validation service for the Root of Trust for Verification (RTV), access controlled and tamper evident or tamper resistant protected storage service for the Root of Trust for Storage (RTS), certification service (providing cryptographic proof that a set of data originates from the RTS) for the Root of Trust for Reporting (RTR).

The term RTM is used in the present document to represent the origin of the Chain of Trust (CoT) (see clause 4.1.2), as the present document is primarily focused on exploring Remote Attestation technologies. Wherever Secure Boot/Local Attestation is instead referenced within the present document, it should be assumed that the origin of the CoT is, in that case, the RTV.

4.1.2 Chain of Trust

A CoT, also known as a Transitive CoT, is used to infer trust in the measurement data of the software component that represents the last link of the chain. Trust is initially only bestowed on the first link in the chain, the Root of Trust for Measurement (RTM).

Starting from the RTM the principle of "first measure and record, then execute" is applied by all software components that are executed on the given platform. It ensures that all software components are measured at load time and cannot tamper with their own measurement procedure. The RTM performs the first measurement, which will be implicitly trusted, because of the defining property of the RTM - immutability (as defined by TCG PC Client Specific Implementation Specification for Conventional BIOS [i.4]). Thus trust can be transferred from the first measurement to the measurement of the last software component in the chain. This process of building a measurement log is also referenced as a Measured Boot process.

When regarded from bottom to top, from the RTM to each of the measurement endpoint software components, this process resembles a tree (of transitive trust), while, when regarded from top to bottom, from the last measured software component to the RTM, it constitutes a CoT.

The CoT is a purely logical construct. It can be explicitly constructed by the Remote Verifier during a Remote Attestation (RA) process as long as the target platform implements either only Measured Boot or both Measured Boot and Secure Boot. For this purpose the data in the measurement log is checked against golden measurements. In case of a match, a new leaf is added to the CoT. Starting from the first mismatch, the data in the measurement log can no longer be trusted and the CoT cannot be expanded further.

When only Secure Boot is implemented by a platform (without Measured Boot), an independent observer (similar to the Remote Verifier used in RA) cannot reconstruct and verify the CoT. It can only trust that the running code was loaded as the last leaf of a properly rooted and locally (on the target platform) constructed CoT.

An example of such a tree/CoT is depicted in Figure 1 (based on TCG Attestation, PTS Protocol: Binding to TNC IF-M [i.5]).

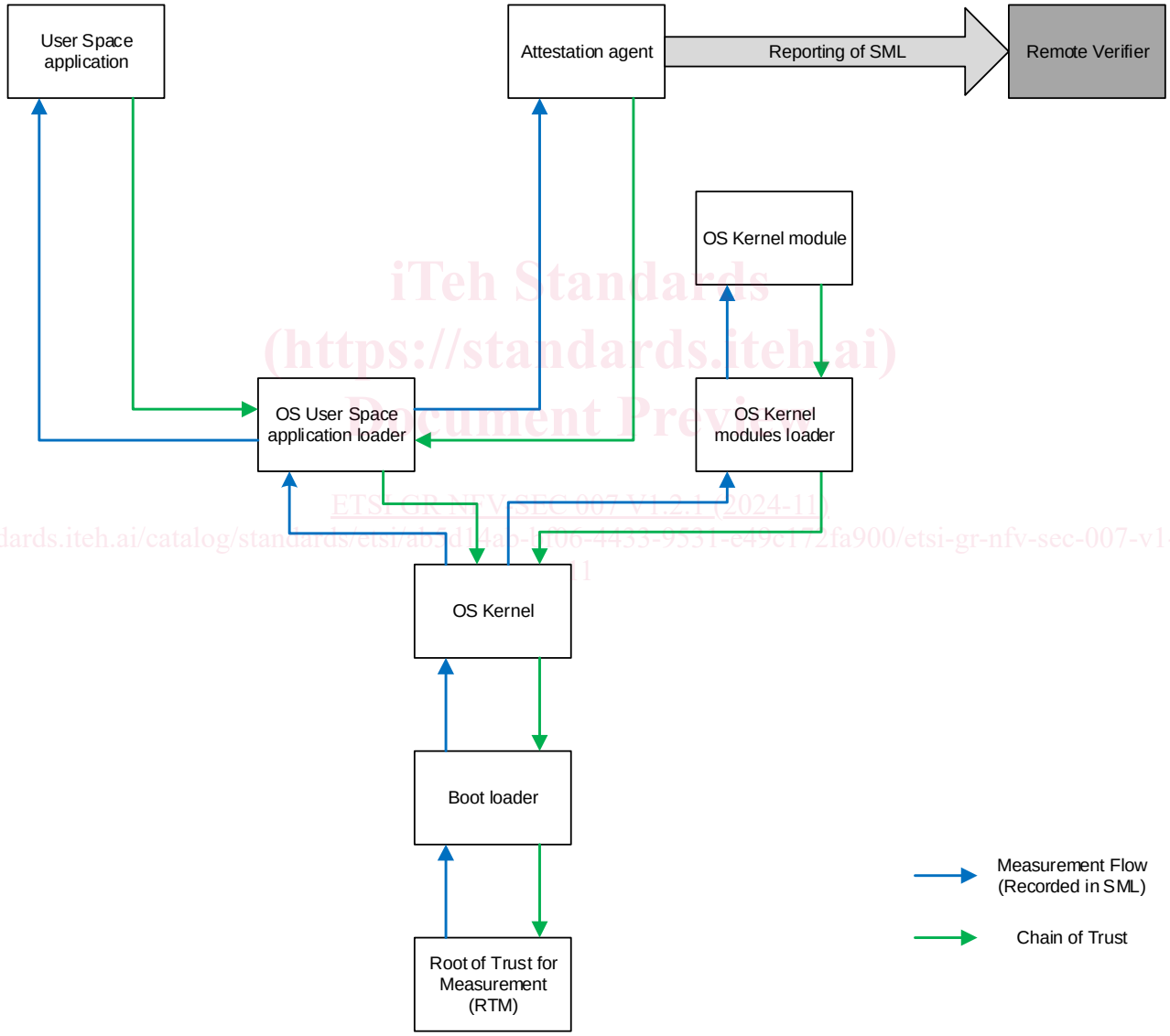

Figure 1: System Services Chain of Trust and Attestation

4.1.3 Attestation

Attestation is the process through which a remote challenger can retrieve verifiable information regarding a platform's integrity state (as described in TCG PC Client Specific Implementation Specification for Conventional BIOS [i.4]). It is also commonly referenced as Remote Attestation, to highlight that the verification of integrity information is performed by an independent party in a different trust domain.

The platform's integrity information is delivered to the remote challenger in the form of a measurements log. However, as specified in TCG PC Client Specific Implementation Specification for Conventional BIOS [i.4], the information in the measurements log alone is not sufficient to enable a trustworthy assessment of the platform's integrity state. The measurement log is generated by the very software running on the platform being assessed. Therefore, trust in data contained in the measurements log is ensured only if:

- A Chain of Trust (CoT) is established from the platform boot up to any given running application being attested (as defined in TCG Attestation, PTS Protocol: Binding to TNC IF-M [i.5]).
- Evidence of measurements log data protection from local tampering is provided.

As explained in clause 4.1.2, any given software component participating to the chain of trust cannot influence its own measurement procedure, as its execution begins only after it has been measured. However, a CoT does not provide assurances that already recorded measurements have not been tampered at a later time. For this purpose a Root of Trust for Reporting (RTR) is required.

A RTR needs to be able to create cryptographic evidence that the data in the measurements log originates from a RTS and has not been tampered.

A TPM (see clause 6.1) is an example of implementation that could provide RTR and RTS by leveraging the specific tampering detection properties of its Platform Configuration Registers (PCR) and issuing signed quotes of their content (as described in TCG Attestation, PTS Protocol: Binding to TNC IF-M [i.5]).

An HSM (see clause 6.2), is another example of implementation that could provide RTR and RTS, using its capability to provide integrity and confidentiality and cryptographic processing.

Upon receiving a measurements log and the appropriate evidence that its contents has not been tampered with, the remote challenger can determine, in a trustworthy manner, the platform's integrity status. For this purpose the remote party uses reference measurements.

4.1.4 Supporting Technologies

4.1.4.1 Measured Boot

As described above, trust in the attestation data is dependent on the establishment of a CoT starting from a RTM. The initialization of this CoT is performed by a measured boot process (according to ETSI GR NFV-SEC 009 [i.6]). The process ensures that all software components starting from the RTM are measured before execution and their measurements recorded in the measurement log, which is integrity protected by the RTR.

Typically, a measured boot covers the measurement of all software components that are executed sequentially, on a linear execution flow, as part of the boot process. This implies constructing the CoT up to, at minimum, the Operating System (OS) kernel. The rest of the CoT from the OS kernel up to any given user space application executed in the system is constructed through load-time measurement.

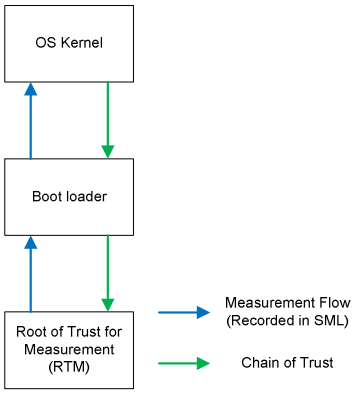

Figure 2: Measured boot CoT

4.1.4.2 Load-Time Measurement

Upon the OS kernel being launched, the execution flow of software components (i.e. applications and kernel modules) is no longer linear. Multiple application and kernel modules can be loaded and executed in parallel and no guarantees as to the order of execution can be provided.

Extending the CoT from the linearly executed boot software components to any given parallel launched user space application can also be accomplished by enforcing the measurement of all applications and modules at load-time, before they are executed, as illustrated in Figure 3. This requires dedicated support, usually within the OS kernel, to ensure that all measurements are properly collected and recorded in the integrity protected SML. It is also sometimes referred to as a "Measurement Architecture".

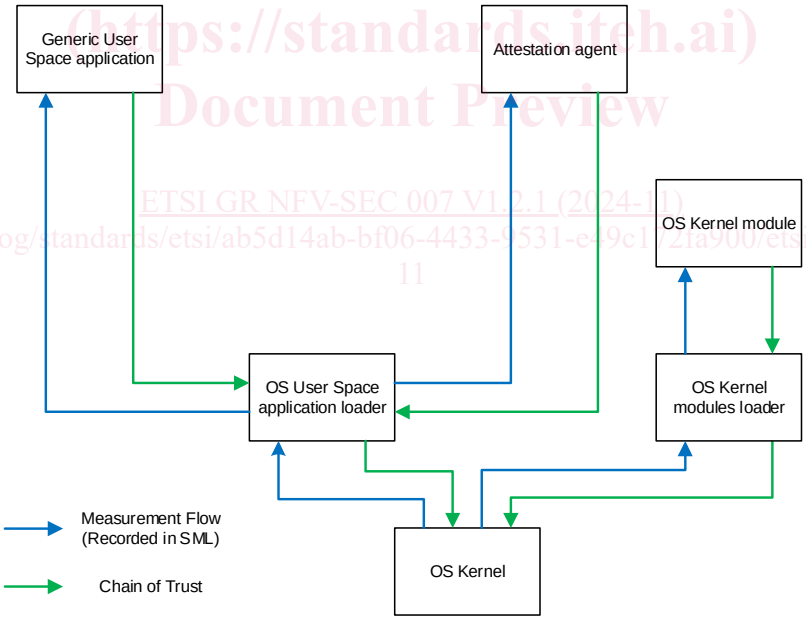

Figure 3: Load-Time CoT

4.2 Enforcement of System Integrity

Attestation provides only the means to remotely detect platform integrity compromise. For cases where local policy enforcement based on integrity information is desired, the principles of Secure Boot, as opposed to Measured Boot or Trusted Boot (as defined by ETSI GR NFV-SEC 003 [i.7]) are more suitable.